The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
10/11/2016

SUBJECT:
Multiple Vulnerabilities in Adobe Acrobat and Adobe Reader Could Allow for Arbitrary Code Execution (APSB16-33)

OVERVIEW:
Multiple vulnerabilities in Adobe Acrobat and Adobe Reader could allow for arbitrary code execution. Adobe Acrobat and Reader allow a user to view, create, manipulate, print and manage files in Portable Document Format (PDF). If the current user is logged on with administrative user rights, an attacker could take control of an affected system. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed attacks may cause a denial-of-service condition.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Adobe Acrobat DC for Windows and Macintosh versions prior to 15.020.20039
- Acrobat Reader DC for Windows and Macintosh versions prior to 15.020.20039
- Acrobat DC for Windows and Macintosh versions prior to 15.006.30243
- Adobe Acrobat Reader DC for Windows and Macintosh versions prior to 15.006.30243
- Adobe Acrobat XI for Windows and Macintosh versions prior to 11.0.18
- Adobe Reader XI for Windows and Macintosh versions prior to 11.0.18

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Adobe Acrobat and Reader are prone to multiple vulnerabilities, the most severe of which could allow for arbitrary code execution. The vulnerabilities are as follows:

- Multiple use-after-free vulnerabilities that could lead to code execution (CVE-2016-1089, CVE-2016-1091, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6949, CVE-2016-6952, CVE-2016-6953, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6971, CVE-2016-6979, CVE-2016-6988, CVE-2016-6993).
- Multiple heap buffer overflow vulnerabilities that could lead to code execution (CVE-2016-6939, CVE-2016-6994).
- Multiple memory corruption vulnerabilities that could lead to code execution (CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6947, CVE-2016-6948, CVE-2016-6950, CVE-2016-6951, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6959, CVE-2016-6960, CVE-2016-6966, CVE-2016-6970, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, CVE-2016-7019).
- Multiple methods to bypass restrictions on Javascript API execution (CVE-2016-6957).
- A security bypass vulnerability (CVE-2016-6958).
- An integer overflow vulnerability that could lead to code execution (CVE-2016-6999).

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed attacks may result in a denial-of-service condition.

RECOMMENDATIONS:
The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.

REFERENCES:
Adobe:
https://helpx.adobe.com/security/products/acrobat/apsb16-33.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1089
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1091
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6939
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6940
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6941

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6942
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6943
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6944
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6945
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6946
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6947
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6948
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6949
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6950
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6951
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6952
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6953
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6954
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6955
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6956
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6957
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6958
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6959
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6960
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6961
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6962
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6963
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6964
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6965
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6966
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6967
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6968
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6969
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6970
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6971
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6972
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6973
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6974
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6975
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6976
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6977
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6978
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6979
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6988
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6993
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6994
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6995
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6996
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6997
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6998
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6999
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7000
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7001

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7002
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7003
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7004
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7005
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7006
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7007
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7008
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7009
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7010
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7011
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7012
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7013
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7014
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7015
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7016
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7017
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7018
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7019